Diese Kopfleiste bitte unbedingt ausfüllen!

Familienname, Vorname (bitte durch eine Leerspalte trennen)

Bereich	Berufsnummer	IHK-Nummer	Prüflingsnummer
7 0	1 2 0 2		
Sp. 1-2	Sp. 3-6	Sp. 7-9	Sp. 10-14

Termin: Mittwoch, 24. November 2021

IHK

Abschlussprüfung Winter 2021/22

1202

2 Analyse und Entwicklung von Netzwerken

Fachinformatiker
Fachinformatikerin
Systemintegration (AO 2020)

Teil 2 der Abschlussprüfung

4 Aufgaben

90 Minuten Prüfungszeit

100 Punkte

Hinweis:
Bei der Bearbeitung der Aufgaben ist von einem gewöhnlichen Geschäftsbetrieb auszugehen, der **nicht** durch die COVID-19-Pandemie beeinflusst bzw. durch entsprechende behördliche Verfügungen eingeschränkt ist.

Bearbeitungshinweise

1. Bevor Sie mit der Bearbeitung der Aufgaben beginnen, überprüfen Sie bitte die **Vollständigkeit** dieses Aufgabensatzes. Die Anzahl der zu bearbeitenden Aufgaben ist auf dem Deckblatt links angegeben. Wenden Sie sich bei Unstimmigkeiten sofort an die Aufsicht, weil Reklamationen am Ende der Prüfung nicht anerkannt werden können.
2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgaben** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Nebenrechnungen/Hilfsaufzeichnungen** können Sie das im Aufgabensatz enthaltene Konzeptpapier verwenden. Dieses muss vor der Bearbeitung der Aufgaben herausgetrennt werden. Bewertet werden jedoch nur Ihre Eintragungen im Aufgabensatz.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen.

1. Aufg.	Punkte	2. Aufg.	Punkte	3. Aufg.	Punkte	4. Aufg.	Punkte
	15 16		17 18		19 20		21 22

Prüfungszeit ___ (23)

Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Gesamtpunktzahl ___ (24 25 26)

Prüfungsort, Datum

Unterschrift

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen.
Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2021 – Alle Rechte vorbehalten!

Die Aufgaben 1 bis 4 beziehen sich auf die folgende Ausgangssituation:

Sie sind Mitarbeiter/-in bei der Professional-Services GmbH, die IT-Lösungen für mittelständische Unternehmen anbietet. Die überregionale Bäckereikette vollKorn GmbH erteilt den Auftrag, die netzwerktechnische Anbindung neuer Filialen an die Zentrale in Köln zu realisieren.

In diesem Zusammenhang sollen Sie folgende vier Aufgaben bearbeiten:
1. Aufgabe: Netzwerk erweitern
2. Aufgabe: WLAN einrichten
3. Aufgabe: Netzwerkverkehr absichern
4. Aufgabe: Netzwerk-Monitoring einführen

Korrekturrand

1. Aufgabe (30 Punkte)

Dem neuen Standort der vollKorn GmbH in Erfurt ist das Subnetz 172.16.102.0 /24 zugewiesen worden. Es ist über zwei Standleitungen mit der Zentrale in Köln sowie mit Berlin verbunden (siehe Netzwerkplan in der perforierten Anlage).

a) Ihre Aufgabe innerhalb der Professional-Services GmbH ist es, für den Standort Erfurt Subnetze für die drei Abteilungen und den administrativen Bereich (IT) zu bilden. Die Größe der Subnetze soll an die Anzahl der maximal benötigten Adressen im Hostbereich angepasst werden, sodass möglichst wenige Adressen verschwendet werden. Der freie Adressblock (falls vorhanden) muss am Ende des Netzwerks liegen.

Ergänzen Sie die folgende Tabelle. 8 Punkte

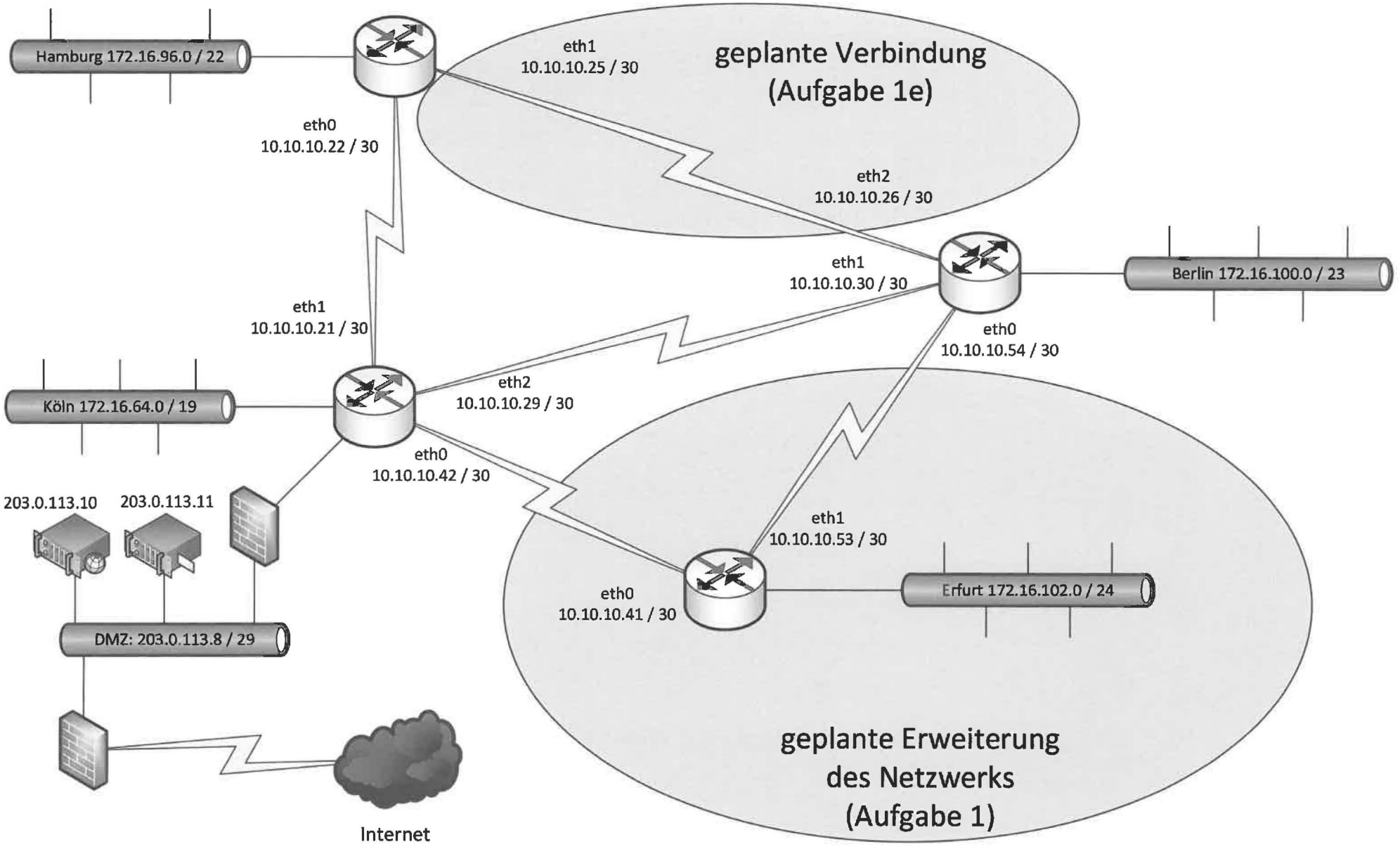
Bereich	Anzahl Hosts	Netzadresse	Subnetzmaske (dezimal)
Abteilung 1	80		
Abteilung 2	50		
Abteilung 3	20		
IT	10		

b) Richten Sie auf dem Router Erfurt die statischen Routen zu den Netzen in Köln, Köln DMZ, Hamburg und Berlin mit minimalen Hops ein. Netzwerkverkehr zum Internet soll ebenfalls möglich sein. Die IPv4-Adressen und Router-Schnittstellen sind dem Netzplan zu entnehmen.
Beachten Sie, dass die direkte Verbindung zwischen Hamburg und Berlin aktuell noch nicht zur Verfügung steht.

Ergänzen Sie die folgende Router-Tabelle um die statischen Routing-Einträge. (Direkt angeschlossene Netze müssen nicht ergänzt werden.) 6 Punkte

Router-Tabelle Erfurt

Netzwerk	Subnetzmaske (dezimal)	Schnittstelle	Next-Hop



Dieses Blatt kann an der Perforation aus dem Aufgabensatz herausgetrennt werden!

Korrekturrand

c) Die vollKorn GmbH nutzt am Standort Köln in einer DMZ einen Webserver, welcher seinen Datenverkehr über TLS verschlüsselt, sowie einen E-Mail-Server, welcher eingehenden SMTP (unverschlüsselt und verschlüsselt) und IMAP (verschlüsselt) Traffic akzeptieren soll.

Ergänzen Sie die folgenden SPI-Firewall-Regeln für den eingehenden Netzwerkverkehr an der äußeren Firewall. 6 Punkte

Richtung	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Protokoll	Regel
	any	203.0.113.10	any			
eingehend	any	203.0.113.11				accept
eingehend			any	993 (IMAP TLS)		
		203.0.113.11		465 (SMTP TLS)		
	any		any	587 (SMTP STARTTLS)	TCP	accept
eingehend						drop

d) Der Support der internen Firewall ist ausgelaufen, daher muss diese ersetzt werden. Es wird darüber nachgedacht, eine „Next Generation Firewall" anzuschaffen.

Erläutern Sie zwei Vorteile, die durch den Einsatz einer solchen Firewall im Vergleich zu einem klassischen Paket-Filter entstehen. 4 Punkte

e) Zwischen den Standorten Hamburg und Berlin besteht nun eine Direktverbindung. Im Zuge der Inbetriebnahme dieser Verbindung wird geprüft, ob das interne Routing von „statisch" auf „dynamisch" umgestellt werden sollte.

Entscheiden Sie sich für eines der beiden Routing-Verfahren und begründen Sie Ihre Entscheidung anhand von zwei Argumenten. 6 Punkte

2. Aufgabe (21 Punkte)

Korrekturrand

Am neuen Standort in Erfurt soll zukünftig auch WLAN für die Anbindung verschiedener interner Netzwerkgeräte sowie für einen Gastzugang für Besucher zur Verfügung gestellt werden. Eine professionelle Ausleuchtung der Räume hat ergeben, dass acht Accesspoints notwendig sind. Der vorhandene WLAN-Controller in Köln soll auch hierfür verwendet werden.

a) Erläutern Sie je eine Aufgabe der folgenden Geräte. 4 Punkte

Accesspoint	
WLAN-Controller	

b) Zur Verschlüsselung der Daten wird WPA2 eingesetzt, welches in den Varianten „WPA2-PSK" und „WPA2-Enterprise" eingesetzt werden kann.

Entscheiden Sie sich für den Einsatz einer der beiden Varianten für die Mitarbeiter der Filiale Erfurt und begründen Sie Ihre Entscheidung. 4 Punkte

c) Neben den beiden oben genannten Geräten Accesspoint und WLAN-Controller wird für den Betrieb des WLANs ein RADIUS-Server eingesetzt. Dessen Aufgaben werden häufig mit der Abkürzung AAA oder Triple-A beschrieben.

Benennen Sie diese Abkürzungen und erläutern Sie ihre Aufgabe und Funktion in einer WLAN-Infrastruktur. 3 Punkte

d) Für Gäste soll ein eigenes WLAN zur Verfügung gestellt werden. Der Zugriff darauf soll über ein WLAN-Ticketsystem (Voucher) mit Zugangsportal geregelt werden.

Erläutern Sie, was man darunter versteht und nennen Sie zwei Vorteile, die ein solches Ticketsystem für den Gastgeber bietet. 4 Punkte

Korrekturrand

e) Die acht Accesspoints wurden bereits angeschafft und sollen über PoE betrieben werden. Folgender Auszug aus dem Datenblatt der Accesspoints liegt vor:

Frequenz	2,4 GHz und 5 GHz
Wireless-Modus	802.11 ac (4x4)
Max. Durchsatz (theoretisch)	1.700 Mbit/s
Leistungsaufnahme PoE+	17,9 Watt
Sicherheit	WPA-3
Anschluss	1 x RJ45 1 / 2,5 Gbit/s 1 x RJ45 1 Gbit/s (PoE+)

Für den Betrieb der Accesspoints soll ein Switch beschafft werden. Der Switch soll an den Core Switch angeschlossen werden. Dazu werden die Datenblätter der folgenden drei Switche verglichen:

	Switch A	**Switch B**	**Switch C**
Anzahl Ports RJ45	8 x 1 Gbit/s	8 x 2,5 Gbit/s	24 x 1 Gbit/s
Anzahl Ports SFP+	0	2	2
PoE+	8 x	2 x	24 x
PoE-Leistungsbudget	250 Watt	60 Watt	180 Watt

Prüfen und begründen Sie, welche der genannten Switche für den Aufbau und Betrieb des WLANs **NICHT** in Frage kommen.

6 Punkte

3. Aufgabe (21 Punkte)

Die Zugriffe auf den Webserver der vollKorn GmbH erfolgen ausschließlich per https. Hierbei wird auf der Transportschicht TLS1.3 verwendet. Sie werden gebeten, einige Sicherheitsaspekte dieser Verbindungsart (TLS) zu erläutern.

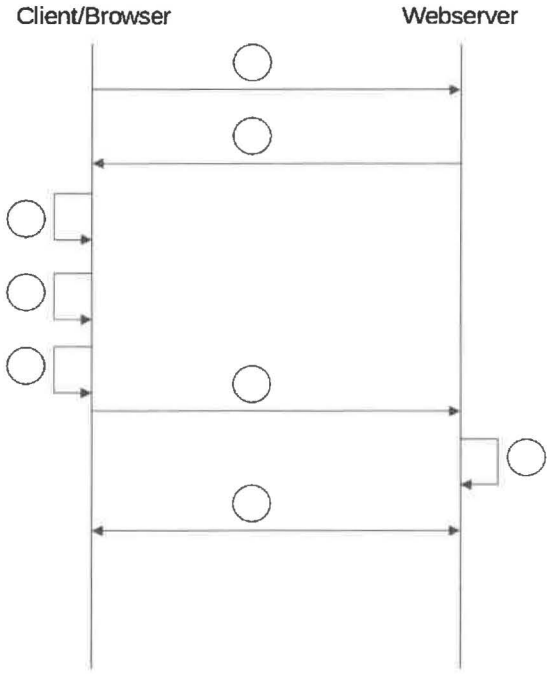
a) Zur Authentifizierung des Webzugangs werden Zertifikate nach X.509 verwendet.

Nennen Sie vier Inhalte, die ein solches Zertifikat enthält. 4 Punkte

Fortsetzung 3. Aufgabe →

Korrekturrand

b) Ergänzen Sie folgendes Sequenzdiagramm, indem Sie die Buchstaben für die folgenden Inhalte an den entsprechenden Stellen in die Kreise eintragen. 8 Punkte



A – AES-verschlüsselte Datenübertragung
B – Entschlüsseln des AES Session Keys
C – Generieren eines AES Session Keys
D – Übergabe des verschlüsselten AES Session Keys
E – Übergabe des Zertifikates inklusive Public Encryption Key
F – Überprüfung des Zertifikates mit Public Decryption Key der CA
G – Verbindungsanfrage
H – Verschlüsseln des AES Session Keys mit Public Encryption Key

c) Bei TLS wird ein hybrides Verschlüsselungsverfahren eingesetzt.

Erläutern Sie den Vorteil eines solchen Verfahrens gegenüber einem nicht hybriden Verfahren. 6 Punkte

d) Eine AES verschlüsselte Verbindung zwischen Client und Server nach TLS 1.3 wurde nun erfolgreich aufgebaut.

Welche Information über das Server-Zertifikat besitzt der Client nach der Überprüfung mithilfe des entsprechenden Stamm-Zertifikats? 3 Punkte

4. Aufgabe (28 Punkte)

Korrekturrand

Mithilfe eines Netzwerk-Monitorings soll der Betrieb des Netzwerkes optimiert werden.

a) Das Netzwerk-Monitoring basiert auf dem Simple Network Management Protokoll (SNMP).

aa) An einer Netzwerkkomponente soll die Systemtemperatur abgefragt werden.

Sie setzen folgenden Befehl ab:

```
C:\snmpget -v 2c -c public 172.16.102.1 1.3.6.1.4.1.{HerstellerID}.
{SensorID-Temp}
```

und erhalten folgende Ausgabe:

```
1.3.6.1.4.1.{HerstellerID}.{SensorID-Temp} = Integer 38
```

Ergänzen Sie die Tabelle um zwei weitere Werte, die sich per SNMP von Netzwerk-Geräten (z. B. Drucker, Server, Router, Serverschrank) auslesen lassen. 6 Punkte

Auszulesender Wert	**Datentyp**	**Beispielhafter Rückgabewert**
Systemtemperatur (SensorID-Temp)	Integer	38 Grad Celsius

ab) Beschreiben Sie den Nachteil eines Monitorings über eine get-Request (snmpget) Abfrage. 3 Punkte

ac) Beschreiben Sie eine Möglichkeit, den Nachteil zu umgehen. 3 Punkte

b) Es erfolgt nun eine Überprüfung verschiedener Funktionen des Netzwerkes.

ba) Sie prüfen als Erstes die Verbindungen ins Internet mittels eines Ping auf die Website www.ihk.de:

Bildschirmausgabe:

```
c:\>ping www.ihk.de

Ping wird ausgeführt für www.ihk.de [141.88.222.152] mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 141.88.222.152:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100% Verlust),
```

Der Aufruf der Website im Browser funktioniert!

Beschreiben Sie eine Ursache, warum der Ping-Befehl dieses Ergebnis liefert. 4 Punkte

Fortsetzung 4. Aufgabe →

Korrekturrand

bb) Sie überprüfen die Namensauflösung im Netzwerk:

```
(1)   c:\>nslookup www.google.de

(2)   Server:  router.local
(3)   Address:  fe80::1
(4)   Nicht autorisierende Antwort:
(5)   Name:    www.google.de
(6)   Addresses:  2a00:1450:4001:815::2003
(7)           216.58.208.35
```

Erklären Sie stichwortartig die Zeilen 2 bis 7. 6 Punkte

Zeile	Erklärung
1	Eingabe des Befehls „nslookup" zur Auflösung des Namens www.google.de
2	
3	
4	
5	
6	
7	

c) Sie überprüfen das Routing ins Internet mittels des Befehls „tracert" (traceroute).

Korrekturrand

```
C:\>tracert www.google.de

Routenverfolgung zu www.google.de [2a00:1450:4001:815::2003]
über maximal 30 Hops:

  1   <1 ms   <1 ms    1 ms  router.local.isp-connect.de [2001:db8::9:200:9cff:fe2e:b2a0]
  2     *       *       *    Zeitüberschreitung der Anforderung.
  3   24 ms   23 ms   24 ms  2a01:598:208:1046:10:255:170:146
  4   24 ms     *     25 ms  2003:0:1806:2700::1
  5   37 ms   37 ms   36 ms  2001:4860:1:1:0:cf8:0:22
  6   37 ms   38 ms   52 ms  2a00:1450:8077::1
  7     *       *       *    Zeitüberschreitung der Anforderung.
  8   37 ms   36 ms   37 ms  2001:4860:0:110c::7
  9   39 ms   39 ms   38 ms  2001:4860::c:4001:e5e9
 10     *       *     39 ms  2001:4860::c:4000:f874
 11   41 ms   38 ms     *    2001:4860::1:0:d0d8
 12   40 ms   41 ms   40 ms  2001:4860:0:1::1abb
 13   38 ms   39 ms   39 ms  fra15s12-in-x03.1e100.net [2a00:1450:4001:815::2003]

Ablaufverfolgung beendet.
```

Nach einigen Minuten prüfen Sie erneut.

```
C:\>tracert www.google.de

Routenverfolgung zu www.google.de [2a00:1450:4001:80b::2003]
über maximal 30 Hops:

  1    1 ms    1 ms    1 ms  router.local.isp-connect.de [2001:db8::9:200:9cff:fe2e:b2a0]
  2     *       *       *    Zeitüberschreitung der Anforderung.
  3   24 ms   24 ms   23 ms  2a01:598:208:1046:10:255:170:146
  4     *       *       *    Zeitüberschreitung der Anforderung.
  5   36 ms   36 ms   37 ms  2001:4860:1:1:0:cf8:0:22
  6   37 ms   37 ms   37 ms  2a00:1450:8094::1
  7     *       *       *    Zeitüberschreitung der Anforderung.
  8     *       *       *    Zeitüberschreitung der Anforderung.
  9   37 ms   37 ms   37 ms  2001:4860::c:4001:e5e9
 10   39 ms   39 ms   39 ms  2001:4860::c:4000:f874
 11   54 ms   39 ms   39 ms  2001:4860::9:4001:31f1
 12   38 ms   39 ms   38 ms  2001:4860:0:11df::1
 13   40 ms   40 ms   40 ms  2001:4860:0:1::216d
 14   38 ms   38 ms   38 ms  fra15s28-in-x03.1e100.net [2a00:1450:4001:80b::2003]

Ablaufverfolgung beendet.
```

ca) Beschreiben Sie, warum folgende Zeile überhaupt ausgegeben wird, obwohl eine Zeitüberschreitung, aber keine IP-Adresse angezeigt wird. 3 Punkte

Zeilennummer * * * Zeitüberschreitung der Anforderung.

cb) Beschreiben Sie eine Ursache, warum die zwei Ausgaben unterschiedlich viele Ausgabezeilen haben. 3 Punkte

bitte wenden!

Abschlussprüfung Winter 2021/22

Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration (AO 2020)
1202

2 Analyse und Entwicklung von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=	100 – 92 Punkte	Note 2	= unter	92 – 81 Punkte
Note 3	= unter	81 – 67 Punkte	Note 4	= unter	67 – 50 Punkte
Note 5	= unter	50 – 30 Punkte	Note 6	= unter	30 – 0 Punkte

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2021 – Alle Rechte vorbehalten!

1. Aufgabe (30 Punkte)

a) 8 Punkte

Bereich	Anzahl Hosts	Netzadresse	Subnetzmaske (dezimal)
Abteilung 1	80	**172.16.102.0**	**255.255.255.128**
Abteilung 2	50	**172.16.102.128**	**255.255.255.192**
Abteilung 3	20	**172.16.102.192**	**255.255.255.224**
IT	10	**172.16.102.224**	**255.255.255.240**

b) 6 Punkte

Netzwerk	Subnetzmaske (dezimal)	Schnittstelle	Next-Hop
172.16.64.0	**255.255.224.0**	**eth0**	**10.10.10.42**
172.16.96.0	**255.255.252.0**	**eth0**	**10.10.10.42**
203.0.113.8	**255.255.255.248**	**eth0**	**10.10.10.42**
172.16.100.0	**255.255.254.0**	**eth1**	**10.10.10.54**
0.0.0.0	**0.0.0.0**	**eth0**	**10.10.10.42**

Die ersten drei Zeilen sind optional, sie können entfallen, wenn die Default-Route (letzte Zeile) richtig gesetzt ist.

c) 6 Punkte

Richtung	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Protokoll	Regel
eingehend	any	203.0.113.10	any	**443**	**TCP**	**accept**
eingehend	any	203.0.113.11	**any**	**25**	**TCP**	accept
eingehend	**any**	**203.0.113.11**	any	993 (IMAP TLS)	**TCP**	**accept**
eingehend	**any**	203.0.113.11	**any**	465 (SMTP TLS)	**TCP**	**accept**
eingehend	any	**203.0.113.11**	any	587 (SMTP STARTTLS)	TCP	accept
eingehend	**any**	**any**	**any**	**any**	**any**	drop

Die Bewertung erfolgt mit 1 Punkt pro Zeile.

d) 4 Punkte
- Intrusion Detection System/Intrusion Prevention System – automatische Erkennung und Abwehr von externen Angriffen (z. B. Abwehr von SYN Flood)
- Schadsoftwareerkennung – Filterung des Datenverkehrs (z. B. eingehende SMTP, Web, SQL, SMB-Verbindungen)
- Anti-Virus-/Anti-SPAM-Filter Mail-Relay – Filterung von eingehenden E-Mails auf bekannte Schadsoftware/SPAM-Merkmale
- QoS-Management – Priorisierung von Netzwerkdiensten (z. B. VoIP) und Bereitstellung abgestufter Bandbreiten für die Datenübertragung
- Payload des Datenstroms – Anwendungen werden identifiziert und können blockiert oder in der Nutzung der Bandbreite eingeschränkt werden.
- u. a.

e) 6 Punkte

Pro „dynamisches Routing"/contra „statisches Routing":
- Routing-Entscheidungen basieren auf dem aktuellen Status des Netzwerkes/Leitungen
- Es wird automatisch nach alternativen Routen gesucht
- Ausfall von einzelnen Leitungen führen nicht zu einem Totalausfall
- Netzwerk dynamisch erweiterbar (neuer Standort)
- Wartungsaufwand geringer, da neue Netzwerke automatisch bei den anderen Standorten konfiguriert werden

Contra „dynamisches Routing"/pro „statisches Routing":
- Höhere Prozessorlast als beim statischen Routing
- Höhere Netzwerkbelastung, da Routinginformationen regelmäßig übertragen werden
- Höherer Aufwand für die Konfiguration und Wartung
- Wissen über Konfiguration von Routing-Protokollen erforderlich

Weitere Argumente auch möglich!

2. Aufgabe (21 Punkte)

a) 4 Punkte

Accesspoint	– Übergang zwischen kabelgebundenem und kabellosem Netzwerk – Strahlt „das WLAN" aus, strahlt die Funksignale/-wellen aus – u. a.
WLAN-Controller	– Zentrale Konfiguration der Accesspoints – Überwachung der Accesspoints – u. a.

b) 4 Punkte
WPA2-PSK verwendet einen gemeinsamen (geheimen) Netzwerkschlüssel für die Verbindung mit dem WLAN, in der Enterprise-Variante kommen benutzerbezogene Zugangsdaten zum Einsatz. Dies ist von Vorteil, wenn bspw. ein Mitarbeiter das Unternehmen verlässt, da dann gezielt dessen Zugangsdaten deaktiviert werden können und das Passwort nicht an allen Geräten im WLAN geändert werden muss.

c) 3 Punkte
Authentifizierung: feststellen, wer der anfragende Benutzer ist (Username/Passwort)
Autorisierung: Zuteilen von Rechten an den Benutzer (Zugriff auf das Netzwerk)
Accounting: Erfassen der Nutzung durch den Benutzer (Zeit, Datenvolumen)

d) 4 Punkte
Die Gäste erhalten jeweils einen Zettel (Ticket) mit Zugangsdaten, die für einen bestimmten Zeitraum gültig sind. Diese müssen sie auf einer Website eingeben, die nach Verbindung mit der angegebenen SSID erscheint.

Vorteile z. B.:
- Durch das Zugangsportal kann vom Gast die Zustimmung zu den Nutzungsbedingungen eingeholten werden.
- Zeitliche Begrenzung
- Volumenabhängige Begrenzung
- Freigabe von Diensten abhängig vom jeweiligen Ticket
- Auf der Portalseite können dem Gast direkt Informationen angeboten werden, z. B. zu eigenen Produkten (Promotion, Umfrage etc.)
- u. a.

e) 6 Punkte
Switch A sollte nicht ausgewählt werden, da die Anzahl Ports nicht ausreichend ist. Es ist mindestens ein Port für den Uplink zu einem anderen Switch erforderlich, denn die Ausleuchtung hat ergeben, dass acht Accesspoints benötigt werden.

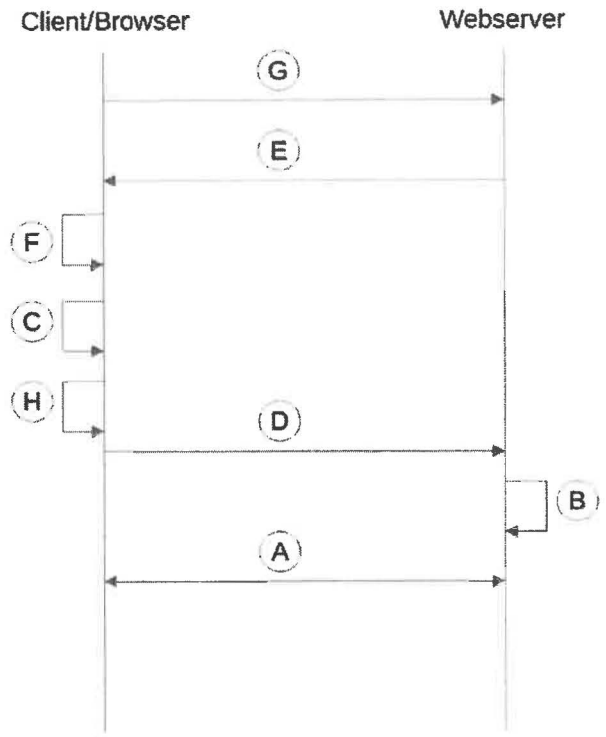
Switch B sollte nicht ausgewählt werden, da die Gesamtleistung über PoE nicht ausreichend für acht Accesspoints à 17,9 Watt ist. Eine Lösung über externe PoE-Injektoren wäre denkbar.

Switch C kann gewählt werden.

3. Aufgabe (21 Punkte)

a) 4 Punkte
- Version
- Name des Zertifikatsinhabers
- Signaturverfahren
- Aussteller des Zertifikats (CA)
- Gültigkeitsdauer
- Verschlüsselungsverfahren
- Öffentlicher Key (encryption) des Zertifikatsinhabers
- u. a.

b) 8 Punkte
Lösungshinweise



c) 6 Punkte
Hybrid: Es wird sowohl ein asym. wie auch ein sym. Verfahren eingesetzt.
Bei TLS bedeutet dies: Beim Verbindungsaufbau/Schlüsselaustausch wird ein asym. Verfahren eingesetzt, nach dem Schlüsselaustausch wird auf ein sym. Verfahren gewechselt.
Asym. Verfahren ist rechenaufwendig, aber kann verwendet werden, ohne vorher ein gemeinsames Schlüsselwort/Geheimnis zu vereinbaren. Dies kann über die unsichere Verbindung erfolgen. Danach wird auf das performantere sym. Verfahren gewechselt.

Weitere Antworten sind möglich.

d) 3 Punkte
Die Gültigkeit des Zertifikates wurde geprüft. Server-Zertifikat lag in der übermittelten Form bei der CA vor und wurde signiert.
HINWEIS: Über die Qualität der Prüfung der Inhalte/Kontaktdaten durch die CA ist nichts ausgesagt.

4. Aufgabe (28 Punkte)

aa) 6 Punkte

Mögliche Lösungen:

Port x Link up	Bool	false/true
Port x Speed	Integer	10 Mbit/sec
Port x Full Duplex	Bool	false/true
Fan Speed	Integer	7.200 U/min
System Load	Float	10 % Last
System online	Bool	false/true
Papierfach leer (bei Drucker)	Bool	false/true
Toner leer (bei Drucker)	Bool	false/true
Standortbezeichnung	String	Netzwerkverteiler 3. OG

Weitere Lösungen sind möglich.

ab) 3 Punkte

Der abgefragte Wert stellt nur den Wert bei der Abfrage dar. Ein außergewöhnlicher Vorfall wie der Ausfall des Lüfters oder steigende Systemtemperatur wird nicht sofort bzw. erst bei der nächsten Abfrage erkannt.

ac) 3 Punkte

Auf dem zu überwachenden Gerät wird z. B. ein Monitoring-Agent (o. Ä.) installiert, der bei Überschreiten eines Schwellwertes eine Nachricht (Trap) an das Monitoringsystem sendet.

ba) 4 Punkte

Auf dem Zielsystem oder auf dem Netzwerkweg ist das Protokoll ICMP durch eine Firewall-Regel gesperrt.

Andere Lösungen sind möglich.

bb) 6 Punkte

(2) Name des antworteten DNS-Servers; hier router.local
(3) IP-Adresse des DNS-Servers; hier IPv6-Adresse fe80::1
(4) „nicht autorisierende Antwort" gibt an, dass es kein offizieller DNS-Server der abgefragten Zone bzw. ein lokaler DNS-Server ist.
(5) Name des abgefragten Servers; hier www.google.de
(6) IPv6 Adresse von www.google.de 2a00:1450:4001:815::2003
(7) IPv4 Adresse von www.google.de 216.58.208.35

ca) 3 Punkte

Da das Feld TTL beim Durchlauf bearbeitet wurde, wird eine Zeile im Trace angezeigt. Das Netzwerkgerät unterstützt keinen Trace/keine Antwort per ICMP oder gibt die Daten nicht zurück.

cb) 3 Punkte

- Der Name wurde auf eine andere IPv6-Adresse aufgelöst (Loadbalancing per DNS). Das Routing zum neuen Zielsystem führt über einen anderen Weg.
- Da das Routing im Internet dynamisch ist, kann sich die Route ändern und die Pakete einen anderen Weg zum Zielsystem nehmen.